Quantum Readiness Roadmap for Businesses

Protecting Your Data in the Post-Quantum Era
vTECH.io | March 2026

Quantum computing is advancing rapidly. Cryptographically relevant quantum computers (CRQCs) could break widely used public-key encryption (RSA, ECC) via Shor's algorithm. The real risk today is Harvest Now, Decrypt Later (HNDL): adversaries are already collecting encrypted data for future decryption.

NIST's post-quantum cryptography (PQC) standards are finalized and ready:

- FIPS 203 – ML-KEM (key encapsulation)
- FIPS 204 – ML-DSA (digital signatures)
- FIPS 205 – SLH-DSA (hash-based signatures)
- HQC (2025 backup for key encapsulation)

Federal timelines (NIST IR 8547, NSM-10) aim for full transition by 2035, with deprecation of vulnerable algorithms starting 2030–2035. Businesses must act now—migration takes 5–10+ years.

Why Start in 2026?

- 2025–2026: Early mandates emerging (e.g., federal procurement guidance, PCI DSS updates).
- HNDL risk is active—long-lived data (IP, health records, financials) is vulnerable.
- Crypto agility is key: Build systems that swap algorithms easily.

Your 5-Phase Quantum Readiness Roadmap

Phase 1: Preparation & Awareness (Now – Q2 2026)

- Form a cross-functional Quantum Transition Team (security, IT, legal, compliance, vendors).
- Educate leadership: Host workshops on quantum risks, HNDL, and PQC basics.
- Align with regulations: Review CNSA 2.0, NSM-10, upcoming EO mandates.
- Engage vendors: Ask for PQC roadmaps and hybrid support timelines.

Phase 2: Cryptographic Inventory & Discovery (Q2–Q4 2026)

- Build a Cryptographic Bill of Materials (CBOM): Scan all systems, apps, hardware, firmware, protocols (TLS, VPNs, code signing, PKI, data-at-rest).
  - Tools: Use automated discovery (e.g., open-source scanners, commercial solutions like Keyfactor or similar).

- Classify assets: Prioritize by data sensitivity, longevity, and exposure (e.g., high-risk = long-term confidentiality needs).
- Identify quantum-vulnerable crypto: RSA/ECDH/ECDSA in use today.

Phase 3: Risk Assessment & Prioritized Planning (Ongoing, Start Q3 2026)

- Assess impact: Map HNDL-vulnerable data; simulate quantum break scenarios.
- Develop migration playbook: Risk-based prioritization (e.g., start with TLS 1.3 hybrids, then PKI/certificates).
- Test hybrid approaches: Combine classical + PQC (e.g., X25519 + ML-KEM) for compatibility.
- Budget & timeline: Plan multi-year rollout; factor in performance (larger keys) and interoperability.

Phase 4: Implementation & Pilots (2027–2029)

- Pilot in low-risk areas: Hybrid TLS, firmware signing, internal VPNs.
- Update libraries/protocols: Integrate NIST PQC into OpenSSL, Bouncy Castle, etc.
- Roll out enterprise-wide: Replace vulnerable algorithms in new systems; retrofit legacy where possible.
- Vendor coordination: Require PQC support in RFPs/contracts.
- Crypto agility: Design systems for future algorithm swaps (e.g., via abstraction layers).

Phase 5: Full Adoption, Monitoring & Optimization (2030+)

- Achieve full PQC compliance: Deprecate vulnerable algorithms per NIST timelines.
- Continuous monitoring: Track NIST/IETF updates, run quantum-risk audits.
- Measure success: Track inventory coverage, hybrid adoption rates, vendor compliance.
- Stay agile: Prepare for additional NIST algorithms or breakthroughs.

Key Challenges & Mitigation Tips

- Performance overhead: Larger keys/signatures—test and optimize (e.g., hybrid modes reduce impact).
- Legacy systems: Phase out or isolate; use gateways/proxies for interim protection.
- Supply chain: Demand PQC transparency from vendors.
- Cost: Spread over years; start with high-value assets.

Next Steps with vTECH.io

We're here to help businesses (and beyond) get quantum-ready. vTECH.io offers:

- Crypto inventory assessments
- Hybrid PQC pilots
- Migration consulting & implementation
- Tailored roadmaps for your industry